National Aeronautics and Space Administration

Mission Operations Assurance

Battling Risk to Preserve Mission Success

Larry Bryant

Jet Propulsion Laboratory, California Institute of Technology

5-6 April 2011

Acknowledgements

- The real authors of this material are:
  - Matt Landano
  - Helmut Partma
  - Grant Faris
  - Khanara Ellers
  - Jose Macias
  - Matt Keuneke

RISK – THE CONTINUING THREAT

What is Mission Success?

MEETING LEVEL 1 REQUIREMENTS

WITHIN COST AND SCHEDULE

WITH ACCEPTABLE RISK AND

DOING IT SAFELY!

What is Risk?

Risk is the likelihood of an undesirable event/outcome occurring AND the severity of the consequences of the occurrence. Risks are classified in the broad areas of implementation and mission risk.

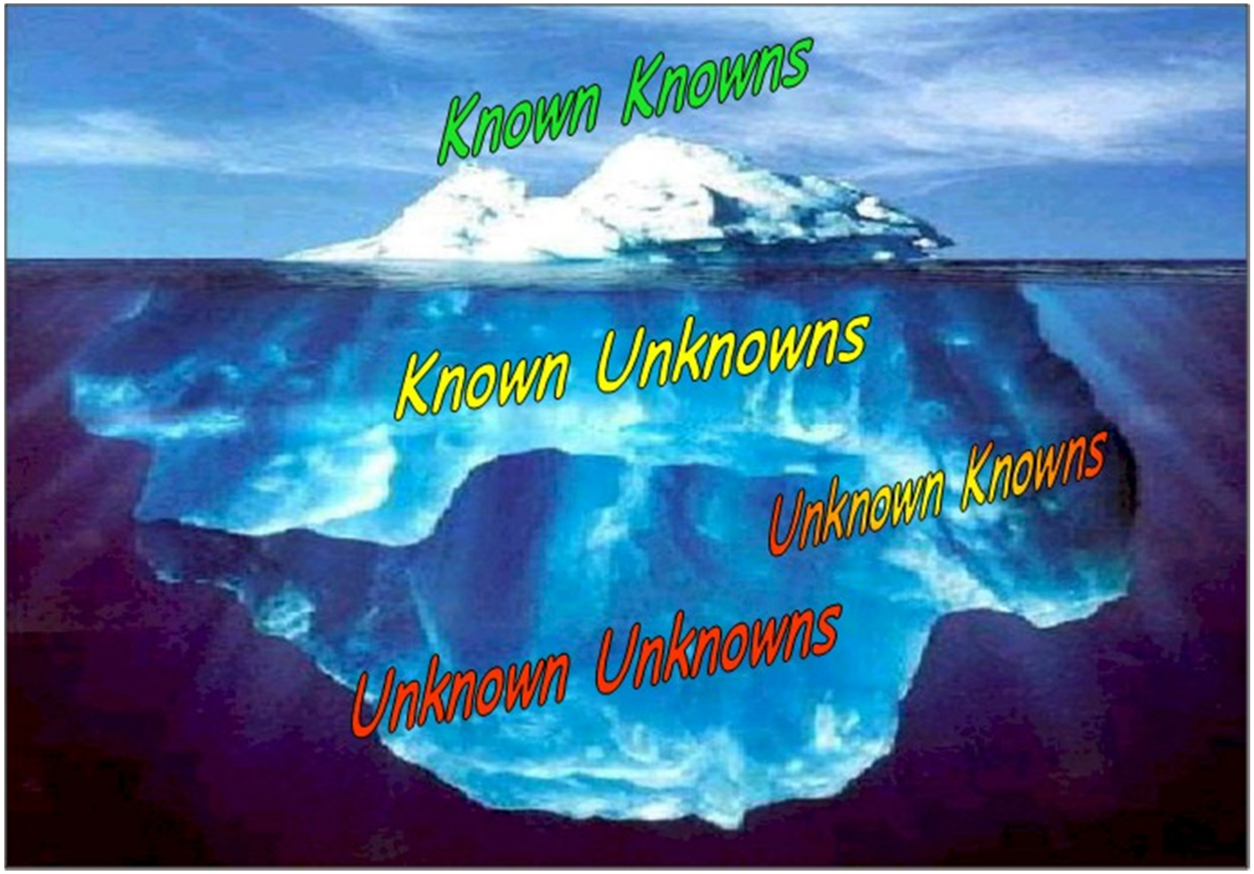
- **Implementation risk addresses cost, schedule, technical and/or programmatic threats.**
- **Mission risk addresses the mission success criteria.**
- **Likelihood is characterized by two major parameters – conditions and window of vulnerability.**
- **Consequence is characterized as either mission impact or implementation impact, and by the set of possible outcomes should the risk item occur.**

Where do Risks Come From?

Experience indicates that risks are derived from several root causes:

- Unsettled definition of mission Level 1 requirements, priorities and full/minimum success criteria
- Incomplete understanding of the driving mission/system requirements, including the impact of mission time-critical activities
- Lack of sufficient margins (technical and programmatic)
- Unsubstantiated assumptions (which are usually optimistic)
- Incomplete identification of key risks and mitigation options
- Unsubstantiated optimism of the capabilities of the project team and/or its contractors/partners
- **Unknown Unknowns**

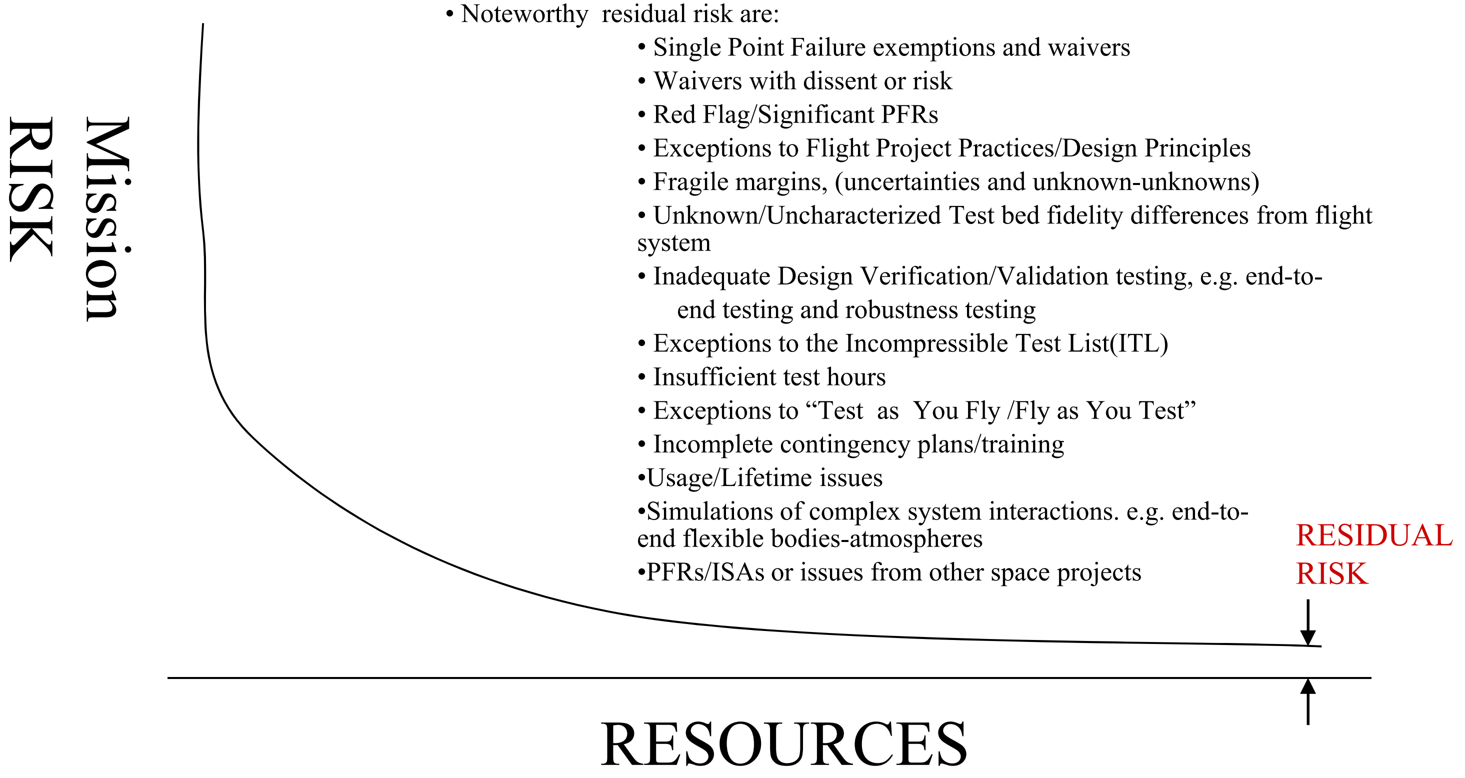
The Risk Iceberg



RISK vs. RESOURCES ILLUSTRATION

CAN NEVER ELIMINATE ALL RISK

- **Residual risk is the risk that remains after mitigation actions have been taken, e.g., H/W, S/W, procedures, sequences, contingency plans and training.**
- Noteworthy residual risk are:
  - Single Point Failure exemptions and waivers
  - Waivers with dissent or risk
  - Red Flag/Significant PFRs
  - Exceptions to Flight Project Practices/Design Principles
  - Fragile margins, (uncertainties and unknown-unknowns)
  - Unknown/Uncharacterized Test bed fidelity differences from flight system
  - Inadequate Design Verification/Validation testing, e.g. end-to-end testing and robustness testing
  - Exceptions to the Incompressible Test List(ITL)
  - Insufficient test hours
  - Exceptions to “Test as You Fly /Fly as You Test”
  - Incomplete contingency plans/training
  - Usage/Lifetime issues
  - Simulations of complex system interactions. e.g. end-to-end flexible bodies-atmospheres
  - PFRs/ISAs or issues from other space projects



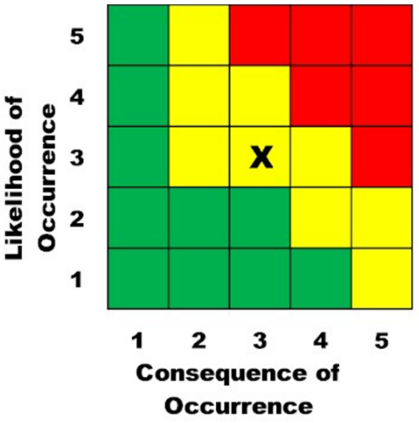
Key Characteristics of JPL (Deep) Space Missions Contributing to Risk

- Challenging One-of-a-kind
- Long Life
- Complex Missions and Payloads
- Extreme Environments (e.g. Mars surface, space and planetary radiation)
- Time-critical Mission Activities
- Long Communication Distances
- Cost and Schedule Constrained

Rating Risk, the 5x5

Likelihood

5	Very High
4	High
3	Moderate
2	Low
1	Very Low



5	🟩	🟨	🟥	🟥	🟥
4	🟩	🟨	🟨	🟥	🟥
3	🟩	🟨	🟨 X	🟨	🟥
2	🟩	🟩	🟩	🟨	🟨
1	🟩	🟩	🟩	🟩	🟨
	1	2	3	4	5

Mission Consequence

5	Mission failure
4	Significant reduction in mission return
3	Moderate reduction in mission return
2	Small reduction in mission return
1	Minimal (or no) impact to mission

Risk Likelihood

Things to Consider in assessing Likelihood of Occurrence

Conditions

- What events/states are needed to enable the risk, e.g.
  - Require a single event/state or multiple independent events/states?
  - Does a single event trigger or cascade into multiple events?
  - Are the events/states transient or steady state?
  - Are the events/states driven by environments?
  - Can events/states be induced by ground errors?
  - Other?

Window of Vulnerability

- What is time duration of the vulnerability period?
  - During Launch phase, Entry/Descent/Landing phase, Orbit Insertion phase, or entire mission?
  - Is the time in millisecs, secs, hours, ...?

Risk Consequence

- The consequence of a risk occurring can vary from negligible to mission degrading to mission catastrophic.
- Assessing consequence requires a functional understanding of the system design, mission objectives, priorities and requirements e.g.:
  - Do consequences threaten personnel/environmental safety?
  - Do consequences threaten flight system health/safety?
  - Do consequences threaten the safe, reliable completion of mission time-critical events?
  - Can ground interaction be applied to preserve flight system health/safety or the safe, reliable completion of time-critical mission activity?
  - Do consequences result in a total loss or degradation of mission return?
  - Do consequences vary with mission phase? e.g. launch, cruise, EDL, orbit insertion.

RISK TRADES, A BALANCING ACT

Approach

- **To provide an independent Mission Assurance assessment of the Project Options for dealing with the approaching conditions/event.**
- **Review the Key areas/events to identify major risk Items: (such as)**
  - Spacecraft safing history, especially during critical times
  - Maintaining redundant/backup capability
  - Swapping from a nominally performing subsystem
  - Flight Software changes
  - Hardware vulnerability
  - Schedule/resource impacts
  - First time in-flight event
- **Recommend an option based on the risk drivers**

Telecom Configuration

- **Downlink lost 8.5 dB output for a period of ~6weeks. The risk mitigation recommended was to stop using the waveguide transfer switch (WGTS) (FOD suspected).**
- **TWTA-A helix current showed an increasing trend. The risk mitigation was to select TWTA-B as the prime TWTA.**
- **Approach and encounter attitudes require use of two different antennas, thus, either the waveguide transfer switch must be used or the TWTAs must be swapped.**

Telecom Configuration Review Areas

- Telemetry visibility during Closest Approach
- Hardware vulnerability
- Schedule/resource impacts
- First time in-flight event

Closest Approach Telecom Options

Risk Drivers	Switch TWTAs	Switch the WGTS	Operate both TWTAs Simultaneously
Telemetry Visibility during C/A	5 Minute Gap starting at C/A + 2 minutes	Full Visibility	Full Visibility
Hardware vulnerability	Swapped nine times between TWTA-A and TWTA-B during extended mission, none during the prime mission (If TWTA fails, FP will swap to the redundant TWTA by exercising the WGTS).	Not recommended by Telecom Anomaly Review Team due to risk of FOD jamming the WGTS resulting in potential loss of mission (WGTS operated 9 times after anomalous 8 dB power drop on TWTA-B prior to determination of FOD as most probable cause).	Initial assessment – feasible from a power perspective, additional analysis needed from a thermal perspective.
Schedule/Resource Impacts	Minimal impact to Sequence development & testing (CURRENT BASELINE)	Minimal impact to Sequence development & testing if implemented in the near-term	Moderate/severe - Sequence development, analysis & testing more complex (in-flight demo, extensive analysis)
In-flight First Time Event	No – Done numerous times in flight	No – Done many times in flight	Yes – Never done in-flight

Mission Assurance Recommendation:

On risk balance, switch the TWTAs which maximizes the likelihood of mission success while accepting a 5 minute telemetry gap starting at closest approach plus 2 minutes.

RCS Thruster Issue

- Two of the RCS thrusters had exceeded their qualification limits in terms of pulses
- Other spacecraft with similar thrusters had experienced failure (just quit working) at these pulse levels
- Upcoming key events in preparation for and including encounter require significant thruster usage

RCS Thruster Review Areas

- Spacecraft safing during critical times
- Characterizing RCS string 2 performance
- Propellant usage due to degraded thruster
- Maintaining redundant RCS thruster capability
- Swapping from a nominally performing RCS thruster string
- Flight Software changes
- Known Thruster performance

RCS Thruster Options

Risk Drivers	Stay on String 1 RCS Thrusters	Swap to String 2 RCS Thrusters
Spacecraft safing during critical activities (TOA burn, approach TMCs and Encounter) due RCS thruster string 1 failure		++
Likelihood of RCS thruster failure disrupting operations		++
Propellant usage due to degraded RCS thruster string 1		+
Maintaining redundant RCS thruster capability		+
Swapping to RCS string 2 with RCS string 1 performing nominally	+	
Flight Software Changes	+	
Known thruster performance	+	
Legend: + = Risk Driver (Advantages) ++ = Major Risk Driver (Advantages)		

MOA Recommendation

- Mission Assurance Recommendation
  - On risk balance, swapping to string 2 RCS thrusters prior to TOA burn and characterizing their performance is recommended.

Considerations

- Spacecraft Safing during critical activities (TOA burn, approach TMCs and Encounter) due RCS thruster string 1 failure
  - Would cause Safe Mode Entry leading to loss of some or all of comet nucleus images which may result in not meeting Primary Mission science requirement.
- Likelihood of RCS thruster string 1 failure disrupting operations
  - In the event of RCS thruster string 1 failed as we approach or at the encounter, the team will have to react and make real time correction in response to the failure which will result in diverging their attention from encounter design, preparation and execution.
  - Swap now will allow the team operations time on string 2 to characterize performance, understand potential problems and make necessary correction prior to encounter; will also enable the team to focus on Encounter Development/Testing/Execution.

Considerations

- Propellant Usage due to degraded RCS thruster string 1
  - Managing Remaining Propellant is critical for maintaining mission flexibility for Time Of Arrival adjustment and to complete nucleus image playback and perform Look-back Imaging. Flying degraded thruster may result in inefficient propellant usage and increased Flyby targeting errors since accurate Flyby distance required to balance image resolution, delivery errors, and mirror tracking speed.
- Maintaining redundant RCS thruster capability
  - Swapping to string 2 will preserve the remaining life of RCS thruster string 1 which result in maintaining the availability of redundant capability for the Encounter.

IMU & UHF Quandary

- IMU-A and UHF Transceiver-A are nearing end-of-life expectancy
  - No Degradation has been observed yet
  - Neither unit is cross-strapped
  - Both are required for Upcoming Critical Operations
  - A-side since Launch
- IMU
  - 86,585 run time hours to date
  - Expected life ~ 69,000 hours (reached in December 2008)
  - An operating IMU is required for Safe Mode and nominal operations
  - Expect indications of impending failure
- UHF Transceiver
  - 10,552 Power Cycles; 9,392 > 20º C thermal cycles to date
  - Expected life ~ 12,000 > 20º C thermal cycles; expected to be reached in November 2013

Side Swap Options

Risk Drivers	Stay on A-side until H/W fault initiates A side swap	Switch to B-side when A-side IMU shows signs Of degradation	Switch to B-side as soon as practical
MSL EDL/Relay support	Possible disruption of MSL support	May not have adequate time to prepare for MSL support given other flight team activities (Phasing activities, OTM, ORTs)	Most time to prepare for MSL support and de-conflict schedule implications
Side swap hardware risk	Delay unknown side swap hardware risk until you absolutely have to. NOTE: Another mission (commanded to the B-side), Others have swapped sides in operation. Swapped sides numerous times in ATLO.	Delay unknown side swap hardware risk until signs of Side A IMU degradation occurs.	Incurs unknown side swap hardware risk in the near-term.
Spacecraft redundancy	Loss of redundancy. Note: IMU is required to initiate All Stellar mode and for safe mode. UHF transceiver required for relay operations. Unreliable mode could significantly extend UHF transceiver life (required for relay operations).	Possible loss of spacecraft redundancy depending on expected life of the degraded IMU. Note: All stellar mode could significantly extend IMU life. Unreliable mode could significantly extend UHF transceiver life (required for relay operations).	Maintains spacecraft redundancy with an IMU showing no signs of degradation. Note: All stellar mode could significantly extend IMU life. Unreliable mode could significantly extend UHF transceiver life (required for relay operations).

MOA Recap

- Other Considerations:
  - Develop All Stellar Mode and implement as soon as possible.
  - Investigate implementing UHF unreliable mode only as soon as possible.
  - Investigate another orbiter taking over the current relay support
- Mission Assurance Recommendation:
  - On risk balance, given the fact that there is significant uncertainty on when IMU-A will fail, recommend delaying the swap to the B-side until signs of degradation are evident from spacecraft telemetry and accept the risk of relay disruption during high visibility Mars Program activities
  - Additionally, expedite the development of the all stellar mode and implement as soon as possible, as well as look at options to preserve the life of the UHF transceiver on the A-side.

Note: Design Principle 9.4.2 (Rev 4) States: Swapping mission-critical hardware to a redundant element shall be limited to fault recovery actions taken to assure health/ safety and/or meet mission requirements, unless there is observed via telemetry unacceptable degradation of the primary unit, and the risk trade, subject to institutional review, indicates pre-empting the on-board fault protection by ground control to be a prudent approach.

Daytime vs Nighttime

- The plan for atmospheric re-entry and landing had been baselined as a nighttime landing
- Concerns over nighttime operations and recovery crew safety prompted a request to reexamine the risks associated with a nighttime landing vs a daytime landing

Daytime Vs Nighttime Entry Decision Review Areas

- Spacecraft Operations
- Ground Impact Hazard Assessment
- STRATCOM Tracking
- SRC Design Margin
- Ground recovery Operations
- Backup Orbit Considerations

Daytime Vs Nighttime Entry Options

Risk Drivers	Nighttime		Daytime	
	Human Safety	Mission Success	Human Safety	Mission Success
Earth Hazard Avoidance				
Ground Impact Hazard Assessment				
SRC Design Margin				
Ground Station Coverage				
SRC processing time - anomalous				
SRC processing time - nominal				
Backup Orbit Duration				
SRC Release Downlink Data Rate				
STRATCOM Tracking				
Legend: + = Risk Driver (Advantages) ++ = Major Risk Driver (Advantages)				

Daytime Vs Nighttime Entry Options

Risk Drivers	Nighttime		Daytime	
	Human Safety	Mission Success	Human Safety	Mission Success
Earth Hazard Avoidance	++			
Ground Impact Hazard Assessment	++			
SRC Design Margin		++		
Ground Station Coverage	++	++		
SRC processing time - anomalous				++
SRC processing time - nominal				
Backup Orbit Duration		+		
SRC Release Downlink Data Rate		+		
STRATCOM Tracking		+		
Legend: + = Risk Driver (Advantages) ++ = Major Risk Driver (Advantages)				

Daytime Vs Nighttime Entry Decision - Considerations

- Downlink data rate at SRC release higher for nighttime entry than daytime entry - doable at either data rate.
- Dual site coverage for SRC release activities available for nighttime entry (Goldstone - Canberra from E-7 to E-2 Hours), not available for daylight entry (Canberra - Madrid station handover at approximately E-4 hours). From an EDL uplink/downlink reliability perspective, a nighttime entry is more robust.
- From an earth hazard avoidance, nighttime entry has the spacecraft targeted to the earth at E-13 days vs E-30 days for the daytime case. From a human safety perspective, a nighttime entry is more robust.

Daytime Vs Nighttime Entry Considerations

- Ground Impact Hazard Assessment
  - Initial assessment shows a hazard track across 2 states (Utah and Colorado) for the nighttime entry vs a longer hazard track across Canada and multiple states for the daytime entry. There may be political implications for a hazard track over Canada. From a human safety perspective, a nighttime entry is more robust.
- STRATCOM Tracking
  - Tracking resources are more robust for the nighttime entry (visual, IR and radar) than for the daytime entry (radar only). STRATCOM tracking is not required for determining the landing location of the SRC.
- SRC Design Margin
  - The environmental entry conditions are more severe for the daytime entry case (Entry velocity 13.16 km/sec vs 12.45 km/sec). It is estimated that about half of the 25 percent aerothermal margin on the SRC is being used up by going to a daytime vs nighttime entry. From an SRC design margin perspective, a nighttime entry is more robust.

Daytime Vs Nighttime Entry Considerations

- Ground Recovery Operations
  - The time to process the SRC once on the ground would be less for the anomalous hard landing case were the capsule is breached. The concern is that moisture may enter the SRC and come into contact with the Aerogel destroying the Wild 2 comet samples. <u>From a sample return recovery perspective, the daytime entry is more robust</u>

- Backup Orbit Considerations
  - The nighttime and daytime entry enables a backup orbit with manageable Delta-V. Preliminary spacecraft and navigation assets say either option is doable. The nighttime entry has the advantage of a shorter backup orbit (by 2 years) reducing the risk to spacecraft component failures. <u>From a spacecraft longevity perspective, the nighttime entry is more robust.</u>

Daytime vs Nighttime Recap

- Major Risk Drivers
  - The major risk drivers are:
    - Earth avoidance strategy - favors a nighttime entry
    - Ground impact hazard assessment - favors a nighttime entry
    - Redundant ground station coverage - favors a nighttime entry
    - The SRC design margin - favors a nighttime entry
    - The recovery processing time for a breached SRC - favors a daytime entry
- Safety and Mission Assurance Recommendation
  - On risk balance, preserving the SRC design margin by coming in at night and accepting a longer SRC processing time in the event of a breached SRC is recommended.

SUBTLE RISKS REQUIRE MOA FOCUS

Where to Point and Click

What can MOA do?
What can the project do?

- Issue: Immediately after the completion of the comet flyby, it was observed that the nominal center of brightness for the comet was not centered within the camera frame.
- Initial investigation:
  - Autonav trajectory predictions were healthy, with prediction errors that were on the order of a few pixels
  - ADCS control errors were healthy, with peak control errors no more than 10 pixels of error.
- Conclusion: It was realized that the impact offset that was determined for the initial flyby might still active in the ADCS software. Telemetry queries confirmed that this impact offset was never scrubbed, and the offset vector of [-0.2, 1.6, -1.4 km] was in effect during the subsequent flyby. This vector had persisted in ADCS memory for the past 5.5 years, since no cold reboot of the prime computer had been performed, and the offset was not cleaned out of ADCS as part of the End-Of-Mission activities.

Is the Computer Listening

What can MOA do?
What can the project do?

- Issue: An antenna control parameter in one spacecraft control processor differed in value slightly from the same parameter in the other processor.
- Conclusion: The processors operated as hot backups for each other and had a special command to load the antenna parameter into both processors simultaneously. However, when this was attempted, the “backup” processor had entered its contingency (vice normal mode or safe mode) and wasn’t listening to the ground. The ground did not have telemetry visibility into this state and was unaware of the unaccepted command until a full memory readout was conducted some time later.

Open the Oven Door

What can MOA do?
What can the project do?

- Issue: Door Open Execution completed nominally but with a partial deploy of the doors. one door estimated at 40% open. outboard door fully open (outboard – against rails open slightly less than 105 degrees.
- Initial Investigation: Engineering telemetry indicated the appropriate power was applied to the door open mechanism for 5 minutes. Power applied for 5 minutes provides plenty of time for the mechanism to operate.
- Conclusion: Review of the "as built" drawings of the bottom rail, indicate changes requested submitted for incorporation into the final fabrication drawings of the FM bottom rail did not get incorporated into the final piece fabrication. The correction requested was not very obvious via visual inspection. Changes had been made on test article.

OPERATIONAL ERRORS

Proximate, Contributing, Root

- **Proximate Cause** (The event(s) that occurred, including any condition(s) that triggered the undesired outcome.)
- **Contributing Cause** (The event(s) or condition(s) that may have contributed to the occurrence of an undesired outcome but, if eliminated or modified, would not by itself have prevented the occurrence.)
- **Root Cause** (The event(s) or condition(s) that led to the proximate cause and subsequent undesired outcome and, if eliminated, or modified would have prevented the undesired outcome.

A Broken Pipe…

- **Background:** During their prime mission, a Mars lander, which was a UHF relay only mission, needed buffer space on a Mars orbiter. This need had the side-effect of reducing the buffer space available to another Mars mission using relay. An interesting behavior was noted by this mission's uplink team, however, in which the orbiter consistently downlinked more data than the allocated buffer space. Upon investigation this was determined to be the result of the orbiter downlinking to Earth at the same time they were uplinking to the orbiter – in other words a "bent pipe" behavior. On a subsequent sol, the Mission Manager urged the team to take advantage of this behavior by converting an orbiter pass to 256k when normally a lower rate would have been recommended.

- **Result:** 30Mbits of data (which happened to be the drive data) was overwritten when the buffer on the orbiter filled up.

- **Analysis:** As it turned out, the UHF pass with the orbiter performed far better than predicted. In addition, the expected 'bent-pipe" behavior did not seem to occur. Upon investigation it was discovered that the orbiter downlink rate at the time in question was much lower than in the previous instances of "bent-pipe" behavior. This fact was "know-able" but not known to the uplink team at the time the decision was made to modify this pass.

Who Needs a Camera Anyway?

- **Background:** The camera mast actuator had faulted unexpectedly, giving rise to the concern that it might be failing. A campaign of diagnostics was devised to pinpoint the cause of this fault. One part of those diagnostics involved inducing camera mast motion through a high-level command. A capture_image command was generated for this purpose, and since the purpose of this command did not include capturing an image, no camera was specified. Later in the process, Seqgen issued an error concerning this command calling it "nonsensical". The uplink team felt they understood the reason that seqgen issued this error and waived it without further investigation. The offending command was uplinked to the rover.

- **Result:** The intended camera mast motion did not occur.

- **Analysis:** Flight software rejected the "empty" capture_image command.

Rubbing Your Belly While Patting Your Head…

- **Background:** A Mars landed mission has an automated targeting algorithm that is meant to be used post-drive when targeted remote sensing is not possible. In one instance during its checkout period, it was sequenced in a morning block. The Mission Manager asked if it was okay for the algorithm to run concurrently with HGA usage. He was assured by the rover planners that there was no conflict. The algorithm activity during the morning block was subsequently uplinked to the rover.

- **Result:** The algorithm activity failed.

- **Analysis:** The algorithm contains a command, which as a mobility command is not allowed to occur concurrently with HGA usage, and was rejected by flight software.

Where’s . . . ?

Proximate Cause (The event(s) that occurred, including any condition(s) that triggered the undesired outcome.)	
Contributing Cause (The event(s) or condition(s) that may have contributed to the occurrence of an undesired outcome but, if eliminated or modified, would not by itself have prevented the occurrence.)	
Root Cause (The event(s) or condition(s) that led to the proximate cause and subsequent undesired outcome and, if eliminated, or modified would have prevented the undesired outcome.	
Corrective and Preventive Actions (include immediate and long-term).	